UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,967	01/30/2001	Mehdi-Laurent Akkar	AKKAR	2638

1444 7590 03/28/2008

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
03/28/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/771,967	AKKAR ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15-24 and 27-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-24 and 27-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A response was received on 03 January 2008. By this response, Claims 25, 26, and 35 have been canceled. No claims have been amended or added. Claims 15-24 and 27-34 are currently pending in the present application.

Election/Restrictions

2. Applicant's election without traverse of Species B, corresponding to Claims 15-24 and 27-34, in the reply filed on 03 January 2008 is acknowledged.

3. Further, Applicant has cancelled Claims 25, 26, and 35, directed to the inventions of Species A and C, and thereby has elected Species B in this manner, in addition to the explicit election in the above noted response. See MPEP § 818.02(c).

Response to Arguments

4. Applicant's arguments filed 01 October 2007 have been fully considered but they are not persuasive.

Claims 14-33 were rejected under 35 U.S.C. 103(a) as unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). In particular, Applicant argues that the features of the independent claims are not taught or suggested by Kocher and/or Chow (page 14 of the present response); however, it is noted that Kocher and Chow were relied upon in combination with each other and also with applicant admitted prior art to show teachings of the claimed limitations. Further, Applicant argues that "if Kocher teaches that some step is to be conducted randomly, [Kocher] fails to teach or suggest to include randomness in the particular step of selecting to take an operation in a normal state or in a complemented state" (page 14 of the present response); however, the Examiner notes that while Kocher was relied upon for a teaching to make a random determination of operations to perform (see Kocher, column 9, lines 1-13, as previously cited), this was considered in combination with the teaching of Chow of a determination of whether to perform an operation or its complement (see Chow, column 18, line 50-column 19, line 13, as previously cited), and the Examiner maintains that the combination of the two teachings would render the claimed limitation obvious. Additionally, Applicant argues that the cited portion of Kocher "is not a teaching of determining what operation to perform based on a random determination" (page 15 of the present response, citing Kocher, column 9, lines 1-13, where randomized permutations of operations are disclosed). Applicant asserts that although the value R used to determine the permutations is

random, “the operation performed is always the same”. However, the Examiner notes that, by this logic, the operation as claimed is also always the same; just the state of the operation is determined randomly, similarly to the disclosure in Kocher of the order of the operations (i.e. which operation to perform at what time) being determined randomly by the permutation. Therefore, the Examiner fails to appreciate a distinction between the claim language and the teaching in Kocher of determining which operation to perform based on a random determination.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning (page 14 of the response received 01 October 2007), it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Therefore, for the reasons detailed above, the Examiner maintains the rejections, or sets forth new grounds of rejection in reference to the new claims, as set forth below.

Claim Objections

5. The objection to Claim 16 for informalities is withdrawn in light of the amendments to the claim. The potential objection under 37 CFR 1.75 of Claim 32 as a substantial duplicate of Claim 23 is moot in light of the amendments to the claims.

Claim Rejections - 35 USC § 101

6. The rejection of the claims under 35 U.S.C. 101 as directed to non-statutory subject matter is moot in light of the cancellation of Claim 14 and is withdrawn with respect to the remaining claims in light of the amendments to the claims.

Claim Rejections - 35 USC § 112

7. The rejection of Claims 14, 25, and 26 under 35 U.S.C. 112, second paragraph, is moot in light of the cancellation of those claims. The rejection of Claims 15-24 and 27-33 under 35 U.S.C. 112, second paragraph, as indefinite is NOT withdrawn. Although the amendments to the claims have remedied some issues of indefiniteness, the amendments and new claims have also raised new issues of indefiniteness, and other issues noted in the previous Office actions have not been addressed. The claims remain rejected, and new grounds of rejection for the new claims, are set forth herein.

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 15-24 and 27-34 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 34 recites the phrase "authentication cryptographic protocol" in lines 1 and 3; this phrase is generally unclear and narrative. The claim also recites the limitation "during performing this authentication cryptographic protocol" in line 3. The phrase "during performing" is generally unclear. Further, the reference to "this authentication cryptographic protocol" is somewhat uncommon, in particular the use of the pronoun "this". It is not entirely clear if "this" is being used in a manner analogous to "the" or "said" or if a different meaning is intended. This is applicable throughout the claims; for example, in lines 7-8 of Claim 34, it is also applicable to the use of the limitations "this server entity" and "this microcircuit entity". Further, in lines 3-4 of the claim, it is not entirely clear whether the phrase "comprising the steps of" is intended to have as its subject the method of performing a protocol, or the protocol itself, noting that the rules of grammar would suggest the latter from the positioning of the phrases.

Claim 34 also recites the limitation "storing a DES" in line 5. It is not clear how one would store an abstract concept such as an encryption standard. The claim also recites the steps of "having a message exchanged", "having the server entity apply", "having the microcircuit entity determine", and "having the microcircuit card apply". These steps are generally unclear because it is not clear what the subject of the verb "having" is; that is, it is not clear who or what "has" these actions occur.

The claim further recites the limitation "this second chain of operations comprising a succession of operations each corresponding to a corresponding operation in the first chain of operations with each operation of the second chain of operations being the corresponding operation of the first chain of operations either in the same state or in the complemented state" in lines 12-16. First, the repetitious use of the term "corresponding" appears to be redundant and obscures the intended meaning of the limitation. Further, again, the use of "this" is unclear because it is not clear if the term is being used in a manner analogous to "said" or the definite article or if a different meaning is intended. Additionally, there does not appear to be clear antecedent basis for the limitation "the corresponding operation", since there was a reference to "each" corresponding operation previously, implying that there are multiple corresponding operations. Finally, there does not appear to be antecedent basis or other clarifying language for the limitations "the same state" or "the complemented state".

The claim also recites "the step of having the microcircuit entity determine the second chain of operations from the first chain of operations comprising a step of randomly selecting, for at least a part of the second chain of operations corresponding to a corresponding part of the first chain of operations, either this at least a part of the operations of the first chain of operations in a same state as in the first chain of operations, or this at least a part of the first chain of operations in a complemented state" in lines 17-22. First, again, the repetitious use of the term "corresponding" appears to be redundant and obscures the intended meaning of the limitation. Further, again, the use of "this" is unclear because it is not clear if the term is being used in a

manner analogous to "said" or the definite article or if a different meaning is intended. Also, it is not clear what the subject of the verb "comprising" is intended to be; it appears from the placement of the words that it is the first chain of operations that is the subject, but this is generally unclear.

The claim further recites the limitation "at least some of the operations" in line 24. The use of the term "some" is indefinite, because it does not clearly define any specific and definite quantity, nor does it set forth a specific numerical range or provide a definite basis of comparison for determining such a quantity.

Claim 34 additionally recites "the microcircuit card" in line 28. There is insufficient antecedent basis for this limitation in the claim, although it appears that this is intended to refer to the microcircuit entity. Similarly, the claim recites "the microcircuit" in line 30; there is insufficient antecedent basis for this limitation in the claim, although it also appears that this is intended to refer to the microcircuit entity. The claim also recites "the step of having the microcircuit apply this second chain of operations comprising a step of selecting to output…" in lines 32-33. It is not clear what the subject of the verb "comprising" is intended to be. From the placement of the phrase, it appears that "operations" or the "second chain of operations" is the subject, but this is generally unclear. Lastly, the claim recites the limitation "validating the authentication" in line 36. This phrase is generally vague and narrative. All of the above renders Claim 34 indefinite.

Claims 15-19, 27, and 28 each recite the limitation "said corresponding part of the first chain of operations corresponding to the at least a part of the second chain of

operations". There is insufficient antecedent basis for this limitation in the claims, and the repetitious use of "corresponding" obscures the meaning of the phrase.

Claim 16 further recites the limitation "operations of said second chain of operations preceding this operation of bit permutation". First, it is again noted that this use of the term "this" is generally unclear as described above. Further, it is not clear which operations of the second chain, if any, clearly precede or follow any operation of permutation.

Similarly, Claim 19 further recites the limitation "operations of said second chain of operations preceding this operation of transfer". First, it is again noted that this use of the term "this" is generally unclear as described above. Further, it is not clear which operations of the second chain, if any, clearly precede or follow any operation of transfer.

Claim 21 recites the limitation "randomly selecting, for each operation of said series of operations of the first chain of operations, such operation either in a normal state or in a complemented state". It is not clear what the state of the operation is selected for.

Claim 22 recites the limitation "the step of selecting to output as the resultant message the result of the last operation in either in a same state or in a complemented state is decided depending on the state of the complementation counter". This is generally unclear, with particular reference to the phrase "the step of selecting to output… is decided". It is not clear how one would decide a step of selecting. Further,

in the phrase "in either in a same state", it appears that one of the instances of "in" should be deleted.

Claim 23 recites the limitation "the result of the last operation in a same state of in a complemented state". This is generally unclear and narrative.

Claim 29 refers to the step of "having the microcircuit entity determine"; again, as described above, it is not clear what the subject of the verb "having" is; that is, it is not clear who or what "has" these actions occur.

Claim 31 recites the limitation "the step of selecting to output as the resultant message the result of the last operation in either in a same state or in a complemented state is decided depending on the state of the complementation counter". This is generally unclear, with particular reference to the phrase "the step of selecting to output… is decided". It is not clear how one would decide a step of selecting. Further, in the phrase "in either in a same state", it appears that one of the instances of "in" should be deleted.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

> invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 15-24 and 27-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783.

In reference to Claim 34, Applicant admits as prior art a method including storing a first chain of operations that performs DES encryption, exchanging a message between a server entity and a microcircuit entity, the server entity applying a first chain of operations to the message to obtain a server result, the microcircuit entity applying a second chain of operations to the message to obtain a resultant message, comparing the resultant message to the server result, and the server and card mutually authenticating when the server result and resultant message are identical (see page 2, lines 3-11, of Applicant's specification). However, Applicant's admitted prior art does not explicitly disclose determining the second chain of operations as explicitly derived from the first chain, nor that the determination is made by randomly selecting to perform operations of the first chain in either a normal or a complemented state.

Chow discloses a tamper-proof encoding method that can be used with encryption protocols (see the description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50-column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the prior art method by performing operations in either a normal or complemented state, in order to increase the

tamper-resistance and obscurity of computer code (see Chow, column 4, lines 3-9). However, Chow does not explicitly disclose determining whether to perform the operation or its complement based on a random determination.

Kocher discloses a cryptographic protocol in which a chain of operations is carried out (Figures 1 and 2; column 1, line 66-column 2, line 24) and in which operations in the chain can be chosen depending on a random decision (column 9, lines 1-13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method, described in Applicant's admitted prior art and modified by Chow, by including a random determination of whether to perform an operation or its complement, in order to increase the security of a system (see Kocher, column 1, line 66-column 2, line 9).

In reference to Claims 15-18, Kocher further discloses that XOR operations, permutation operations, indexed access to a table, and operations that are stable with respect to XOR can be used as operations in the chain (column 2, line 44-column 3, line 9, especially column 2, lines 44-45). Chow also discloses permutations and indexed access to a table (column 18, lines 43-49; column 19, lines 52-61; column 20, lines 48-53).

In reference to Claim 19, Kocher further discloses that operations that transfer data between memory locations may be performed (column 8, lines 45-57).

In reference to Claims 20 and 21, Chow further discloses that a decision whether to perform an operation or its complement is made for each operation (column 18, line 65-column 19, line 13).

In reference to Claims 22 and 31, Kocher further discloses that new operations are determined based on a random parameter (column 9, lines 7-13, 30-48, and 62-64) and a counter is updated (column 9, lines 25-27).

In reference to Claims 23 and 32, Kocher further discloses that new operations are determined based on a random parameter (column 9, lines 7-13, 30-48, and 62-64) and intermediate responses are transmitted (see column 2, lines 17-19).

In reference to Claims 24 and 33, Kocher further discloses comparing a counter against a threshold value and altering operation based on the comparison (column 9, lines 25-30).

In reference to Claim 27, Kocher further discloses performing operations byte by byte (see column 5, lines 20-27).

In reference to Claim 28, Kocher further discloses performing operations bit by bit (see column 2, line 45; also column 10, lines 51-60). Chow also discloses bit by bit operation (column 18, lines 65-66).

In reference to Claims 29 and 30, Kocher further discloses that the order of execution of operations can be permuted randomly (column 10, lines 51-55).

Conclusion

12. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/ZAD/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137